JUDGE ROBERT J. BRYAN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. DAVID TIPPENS, Defendant.	No. CR16-5110RJB DEFENDANT'S SECOND MOTION TO SUPPRESS EVIDENCE *[Oral Argument Requested]* **NOTED: February 3, 2016**

David Tippens, by and through his attorney, Colin Fieman, moves to suppress all evidence obtained through execution of a warrant at his residence in University Place, Washington. The pretrial motion deadline in this case is January 26, 2017. Trial is scheduled for February 27, 2017.[1]

I. INTRODUCTION

Mr. Tippens' first motion to suppress focused on the global NIT warrant that was issued in the Eastern District of Virginia. This motion addresses the subsequent warrant that was issued a year later to search Mr. Tippens' home in University Place

[1]Although the defense served comprehensive discovery demands on the Government on February 12, 2015, much of the discovery relevant to this motion (including exhibits C, D and E) was disclosed by the prosecution only recently. The Government has offered no explanation for why this evidence was not disclosed prior to the earlier motion deadlines set by the Court.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

and seize his computer. *See* dkt. 37-3 (February 9, 2016, local warrants); exh. B (affidavit in support of 2016 warrants).

The 2016 warrant fails to establish probable cause to believe that evidence or instrumentalities of a crime would be found at that location. The crux of the warrant application is that a visitor known as "candygirl123" used a computer with an IP address assigned to Mr. Tippens' residence in Hawaii to view pictures on the Playpen website in February, 2015.

However, in September 2015, the Chief Legal Counsel for the FBI's Hawaii field office determined that "any legal inferences we can make about SFC Tippens viewing, downloading or manufacturing child pornography is extremely low and tenuous at best." Exh. D. Consistent with this conclusion, the FBI rejected the Army's offer to postpone Mr. Tippens' transfer to Washington and seek a warrant to search his property while it was still in the custody of the Army's shippers.

Approximately five months later, the FBI reversed course and decided to seek a warrant in Washington. No new information is included in the 2016 warrant application; it makes no showing that Mr. Tippens had Internet service at the new residence, let alone a computer; and it offers no particularized facts establishing probable cause to believe that any evidence that may have been found one year earlier and several thousand miles away in Honolulu was likely to be found in University Place.

Moreover, the FBI intentionally or recklessly omitted information that was material to the Magistrate Judge's determination of probable cause. The defense requests a *Franks* hearing on the following four grounds:

First, the affidavit alleges that the user "candygirl123," who was linked to Mr. Tippens' IP address in Hawaii, viewed various graphic pictures on the Playpen web site in February, 2015. However, it does not allege that the visitor took any steps to

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

download or copy pictures or videos. Instead, in order to establish probable cause to believe that illicit pictures or other evidence of a pornography offense would be found on the Hawaii computer, the application alleges that copies of the pictures would have been automatically saved on that computer when "candygirl123" viewed them. *See* exh. B at ¶¶ 33-34. That claim is demonstrably false.

On the regular Internet, copies of web pages that a visitor views are automatically copied onto the computer that is connected to that web page. The opposite is true for the Tor network. As an added privacy and security measure, the Tor browser, unlike regular Internet browsers, is designed to prevent automatic downloading of web pages and related data. Since the affidavit does not allege that there is any evidence (based on Playpen's server records or otherwise) that "candygirl123" saved, posted or distributed any illicit pictures, the FBI affirmatively misled the issuing judge about the downloading and the likelihood of finding evidence at the search location.

The second *Franks* issue undermines the application's attempt to bridge the gap between the time and place where someone visited the Playpen site (Hawaii) and the location of the search (University Place). In this regard, the affidavit relies on a "collector profile" to show that people who view and possess child pornography are likely to keep it for a long time. Exh. B at ¶¶ 43-44.

Apart from the fact that this profile is boilerplate, it is recklessly or intentionally misleading. As the Government itself has explained elsewhere, Tor users are *not* typical Internet users or "collectors." Instead, the Government has characterized Tor users as technically sophisticated, sensitive to security and detection, and attentive to news that may circulate about Internet investigations. Moreover, as already noted, the Tor browser blocks automatic downloads, making the usual assumptions about continuing

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

possession of illicit pictures and related data that might apply to the average Internet user inapplicable to Tor users.

The third *Franks* issue arises from the Government's disclosure of portions of the FBI's investigation file. These records show that in October, 2015, agents obtained a copy of the inventory for the personal property that the Army shipped to Washington for Mr. Tippens. Exh. E. The inventory was prepared by the Army's movers and includes a list of electronic devices, but no computers or digital storage devices are listed on it. The affidavit makes no mention of this fact, and it contains no other facts that might establish the presence of a computer devices at the Washington premises.

Finally, the affiant deliberately or recklessly misled the issuing judge by failing to disclose that the FBI had previously decided that there was insufficient evidence to support a warrant. *See* exh. D. The FBI reached this conclusion in September, 2015, approximately six months after it had collected all of the evidence that it would later rely on for the local warrant. The FBI's assessment of the evidence collected by the NIT was not disclosed to the Magistrate Judge and it is inconsistent with many of the opinions, inferences and conclusions that were presented to her.

II. STATEMENT OF FACTS

A. The Hawaii Investigation

The Court is already familiar with the original NIT warrant issued in the Eastern District of Virginia and the facts leading up to the seizure of the IP address connected to Mr. Tippens' prior residence in Hawaii. *See* dkt. 26 (First Motion to Suppress) at 2-7.

Law enforcement agents had identified the physical location associated with this IP address in March, 2015. Exh. B at ¶ 36. The FBI office in Honolulu opened an investigation into Mr. Tippens in June, 2015, in conjunction with the Army's Criminal Investigation Division (CID). Later the same month, investigators confirmed that Mr. Tippens resided with another adult (his mother) and his two minor daughters.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Concerned about the presence of children at the Hawaii residence, CID immediately began coordinating with the FBI to obtain a warrant and search the house, including use of a "SWAT" team.

For reasons that are unclear, the FBI was slow to respond to CID's requests for information needed to complete a warrant application. Meanwhile, Mr. Tippens was ordered transferred to Joint Base Lewis McChord (JBLM), and the Army packed and shipped his personal property on or about August 31, 2015. On September 22, 2015, shortly before Mr. Tippens was scheduled to leave Hawaii, a JAG Senior Trial Counsel who was involved in the investigation emailed the FBI's lead case agent in Honolulu and others to inform them that the Army could delay his departure and that the Army's shippers still had custody of his property, which had arrived in Washington. Exh. C.

Later the same day, the FBI's Chief Division Counsel in Honolulu responded by acknowledging that "[i]n the past, we usually requested your office to stop someone from transferring to the mainland or overseas, but on this occasion, we are seeking the opposite." Exh. D. The Chief Division Counsel is the FBI's top legal adviser for each field office and his or her responsibilities include "assess[ing] the legal implications of tools, technologies and techniques used by the FBI."[2] According to the Chief Division Counsel in Hawaii, "Currently, any legal inferences we can make about SFC Tippens viewing, downloading or manufacturing child pornography is extremely low and tenuous at best." *Id*. The FBI therefore decided to hand off the investigation to its Seattle office "to continue the investigation into his alleged child pornography activities." *Id.*

On October 1, 2015, the FBI added a copy of the "Government Bill of Lading" for Mr. Tippens' property to his case file. *See* exh. E. The moving company hired by

[2] *See* https://www.fbijobs.gov/career-paths/lega, which describes the Chief Division Counsel's duties and qualifications.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

the Army prepared a detailed inventory. It lists such electronic items as a camera, a printer and a television, but no computers. This fact was not disclosed in the local warrant application.

B. The Washington Search

On February 11, 2016, FBI agents assisted by local law enforcement executed the local search warrant at Mr. Tippens' new home in University Place and, among other property, seized a laptop computer.

The affidavit in support of that warrant states that user "candygirl123" logged on to the FBI's Playpen web site for 26 hours on and before February 28, 2015. Exh. B at ¶ 29. The affidavit links that user to Mr. Tippens' residence in Hawaii through an IP address that had been seized by the FBI's NIT malware and describes various "posts" that the user looked at while on the site. *Id*. at ¶¶ 27-36. The affidavit does not allege that the visitor took any of the additional steps needed to intentionally download and save posts, such as clicking on the "save as" option. The affidavit also does not claim that the user posted any pictures; communicated with anyone about sharing pictures; or otherwise indicated that he or she possessed pornography.

Instead, the affidavit alleges that the user's computer automatically saved copies of the posts he/she had viewed when, "after accessing the post, the user clicked directly on the described image *which would have resulted in downloading* another copy of the image to the user's computer." Exh. A at ¶ 34 (emphasis added).

That statement is false. In truth, the Tor browser is configured to block computers from automatically downloading copies of web pages and pictures that a user views while on the Tor network, along with related browsing data. As explained in the accompanying declaration of Prof. Matthew Miller, the regular Internet and the Tor

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

network work differently when it comes to storing data about user activity and web site visits. *See* exh. A (Prof. Miller's declaration and curriculum vitae).[3]

With the regular Internet, and with common browsers like Internet Explorer, copies of web pages are automatically saved by the computer in a section of its hard drive and memory called the "cache." *Id*. at ¶ 3. Cache files are often fragmentary and temporary; many people are unaware that their computers automatically save some files in the cache; and these files are not listed in saved file directories. It is also relatively difficult to locate and retrieve cache files unless a user knows where to look for them. *Id*. Nevertheless, copies of web pages that are stored in cache files may have evidentiary value and their presence may help support a search warrant.

Computers automatically save "cache" files to improve the speed with which users can browse the Internet and view sites that they revisit. *Id*. at ¶¶ 3(c) and 5. For example, if a user visits the front page of *The New York Times* site in the morning, his or her computer will automatically save all or part of that page in the cache, regardless of whether the viewer wants to save it. If the user decides to check the news again later in the day, the computer can then retrieve a copy of the *New York Times* directly from its cache and update it without having to reload all of the page from the newspaper's server. This direct access to web pages that a user has previously visited increases the speed with which those pages can be displayed again. Over time, cache files may be automatically deleted or overwritten by the computer without its users necessarily knowing that the files were ever on the computer. *Id*. at ¶ 3(d).

The Tor network and its users are different because they prioritize privacy and security over speed. In order to prevent computers from automatically downloading and saving data from Tor sites, the Tor browser is programmed to do the opposite of regular

[3] The testimony of Government expert Prof. Brian Levine referenced in Prof. Miller's declaration at ¶ 8 is from the transcript of Levine's testimony on November 1, 2016, at pages 65-71.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Internet browsers: it blocks computers from automatically storing copies of web pages that a user has visited. *Id*. at ¶¶ 5-6.

Anyone familiar with Tor would know this, since it is part of Tor's special privacy and security features. It is also explained on the Tor project's web site. *See* Exh. A at ¶ 7; *see also* Dkt. 37-1 (NIT warrant application) at ¶ 7 ("Information documenting what Tor is and how it works is provided on the publicly accessible Tor website at www.torproject.org").

Further, the original NIT warrant application refers to this Tor security feature, where it notes that Playpen notified visitors that "[t]his website is not able to see your IP and cannot collect *or send any other form of information to your computer except what you expressly upload*." Dkt. 37-1 (NIT warrant application) at ¶ 13 (emphasis added). The affidavit for the local warrant includes a summary of the very same notification, but it omits the information about information blocking. *Compare* exh. B, ¶ 16 *with* Dkt. 37-1, ¶ 13.

Although the affiant in this case stated that he has specialized training and experience in investigating Internet and computer offenses, and that he had consulted with other agents and experts involved in the Playpen investigation, there is no mention of these Tor security features in his affidavit. *See, e.g.*, exh. B at ¶¶ 3-6. To the contrary, the affiant affirmatively claims that "candygirl123" would have downloaded Playpen images when he or she simply viewed them, even though that would not have occurred.

C. The "Collector Profile"

The affidavit also includes a generic "collector profile." *Id.* at ¶¶ 43-44. It states, *inter alia*, that individuals who "access with intent to view and possess, collect, receive, or distribute" child pornography "may" collect sexual images and use them in a variety of ways; "typically" retain pictures and other media "for many years"; "often" maintain

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

digital collections in a secure environment, "usually" at the collector's residence; and "may" correspond with others and "rarely" destroy their correspondence. *Id*.

The affidavit does not address at all the characteristics, habits, or preferences of Tor users, even though the Government has elsewhere stated that Tor users are technologically sophisticated and not like typical Internet users or "collectors."

For example, in its motions for delayed notification of the NIT searches, the Government stated that "[u]sers of illegal child pornography websites on the Tor network are extremely sensitive to law enforcement infiltration." Exh. F (Requests for Extension of Delayed Notice filed April 3, 2015; June 30, 2015; and September 24, 2015, in the Eastern District of Virginia) at Bates 415, 422 and 430. The Government has also stated that Tor users tend to publicize and share information about law enforcement methods, investigations, and how to conceal or destroy digital evidence. *Id*. This, according to the Government, may result in "flight from prosecution, the destruction of or tampering with evidence and otherwise seriously jeopardize the investigation." *Id*. at 416, 423 and 431.

The court in the Eastern District of Virginia relied on these representations about Tor users, and the time sensitive nature of seizing information from them, when it issued its delayed notice orders. *See* exh. G (EDVA delayed notice orders). None of this information, however, was included in the local affidavit's "collector profile."

II. ARGUMENT

A. This Court Should Grant a *Franks* Hearing Because the FBI Intentionally or Recklessly Misrepresented and Omitted Key Facts.

1. The Applicable Law

In *Franks v. Delaware*, 438 U.S. 154, 156 (1978), the Supreme Court held that where a defendant makes "a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

the affiant in the warrant affidavit," and that statement is material to a finding of probable cause, courts are required to hold a hearing at the defendant's request. The doctrine applies to omissions as well as false statements. *United States v. Stanert*, 762 F.2d 775, 780-81 (9th Cir.), *amended by* 769 F.2d 1410 (1985).

The danger in omissions from an affidavit for search warrant are set forth in *Stanert*:

> The use of deliberately falsified information is not the only way by which police officers can mislead a magistrate when making a probable cause determination. By reporting less than the total story, an affiant can manipulate the inferences a magistrate will draw. To allow a magistrate to be misled in such a manner could denude the probable cause requirement of all real meaning.

762 F.2d at 781.

Given these dangers, a defendant need not demonstrate that a judge would have affirmatively denied the warrant if the true or missing information had been included. Instead, the false or missing information is material even if it would only have led the magistrate to "require[] further information" before deciding whether to grant the warrant. *Liston v. Cnty. of Riverside*, 120 F.3d 965, 974 (9th Cir. 1997), *impliedly overruled on other grounds*, *Saucier v. Katz*, 533 U.S. 194 (2001).

Once a *Franks* violation is established, the remedy is to include the omitted information and exclude the false statements from the affidavit. *United States v. Condo*, 782 F.2d 1502, 1506 (9th Cir. 1986). The district court must then review the "reformed" affidavit and make a *de novo* determination of probable cause, without the usual deference to the issuing magistrate. *United States v. Kelley*, 482 F.3d 1047, 1051 (9th Cir. 2007). In addition, the Supreme Court explicitly precluded application of the "good faith" doctrine to *Franks* violations, for the obvious reason that one does not act in good faith when one recklessly or intentionally excludes material facts from a warrant application. *See United States v. Leon*, 468 U.S. 897, 923 (1984).

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

In this case, there are four reckless or deliberate falsehoods or omissions, each of which standing alone make the reformed affidavit lacking in probable cause, particularly when viewed in conjunction with the lapse of time and distance between the target's alleged activity on Playpen and the search.

2. The First *Franks* Violation: The False Statements About Downloading and Receipt or Possession of Pictures.

The affidavit does not allege that "candygirl123" knowingly or intentionally downloaded child pornography. To the contrary, it describes various times when the visitor looked at pictures on the site, and then alleges that those pictures were downloaded by the visitor's computer as an inevitable function of viewing them. Exh. B, ¶¶ 33-34.

The Government's premise here, as it has been with many other warrant applications, is that "[a]s the [defendant] viewed the images online and enlarged them on his screen, his computer automatically saved copies of the images to his 'internet cache.'" *United States v. Romm*, 455 F.3d 990, 993 (9th Cir. 2006); *see also id.* at 998. (holding that a defendant can be convicted of possessing or receiving child pornography when, "at a minimum," he knows that the images will be automatically saved on his computer and also has "the ability to copy, print, or email the images to others").

Hence, when a computer automatically saves copies of illegal pictures in its "cache," a judge can conclude two things in the typical Internet case. First, illicit pictures are likely to be found on the target computer, even if there is no evidence that its user intended to possess or receive any pictures. Second, the cache pictures may survive over time in a format that allows the user to later retrieve those pictures and print, email or otherwise handle them in ways consistent with actual possession.

With Tor, however, pictures are not automatically saved on a target computer, and there are no cache copies that a user can later retrieve and use. Unlike regular

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Internet browsers, the Tor browser is designed to block automatic downloads. *See* exh. A (Miller Declaration) at ¶¶ 3-7.

Moreover, Tor is popular because of its added security features, and its blocking functions are explained on the Tor project's web site, facts that should be well known to an agent who claims relevant expertise. *Id*. at ¶ 7; Dkt. 37-1 (NIT warrant application) at ¶ 7 (noting that "[i]nformation documenting what Tor is and how it works is provided on the publicly accessible Tor website at ww.torproject.org"). Further, the original NIT warrant refers to this Tor security feature, where it notes that the Playpen home page announces that "[t]his website is not able to see your IP and cannot collect *or send any other form of information to your computer except what you expressly upload*." Dkt. 37-1 (NIT warrant application) at ¶ 13 (emphasis added). As previously noted, the affiant here summarized and quoted parts of the very same notification, but left out the most relevant part. *Compare id. with* exh. B, ¶ 16.

Given the true facts about the computer activity that occurred when visitors were connected to Playpen, there was no probable cause to believe that the pictures described in the affidavit (or any related data) would have been found at Mr. Tippens' home in Hawaii, let alone at his home in Washington a year later. Moreover, the affidavit does not allege that the target visited sites other than Playpen, or offered any other basis for concluding that he or she was in possession of contraband. As a result, the affidavit affirmatively misled the issuing judge by presenting key facts as if this were a regular computer and Internet case, when in fact the Tor network functions very differently.

Finally, the affidavit's failure to disclose these facts was, at a minimum, reckless. First, the affiant claimed that he had relevant technical expertise. Exh. B at ¶¶ 2-4. The application also includes an entire section on Tor without disclosing that it is designed to block automatic downloads. *Id*. at ¶¶ 9-12. Further, as previously noted, the original NIT warrant application references the Tor project web site, which explains

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

the blocking functions, and the home page that the FBI maintained for Playpen refers to that safeguard. And, of course, Tor is largely financed by the Government (which provides up to 90% of its annual funding) and the FBI has designed malware to penetrate Tor's defenses, rendering futile any claim that the FBI was unaware of how downloads on Tor can or cannot occur. The Government also cannot credibly maintain that it was not obligated to present the issuing judge with this information. *See, e.g.*, *United States v. Chesher*, 678 F.2d 1353, 1362 (9th Cir. 1982) (failure of officer having extensive contacts with other investigators to discover that defendant was no longer with Hell's Angels, contrary to assertion in affidavit, constituted sufficient showing of intentional or reckless falsity to warrant *Franks* hearing; reversing denial of hearing); *United States v. Comprehensive Drug Testing, Inc*. 621 F.3d 1162, 1178 (9th Cir. 2010) (Kozinski, J., concurring) (CDT) ("a lack of candor in [any] aspect of the warrant application must bear heavily against the government in the calculus of any subsequent motion to return or suppress the seized data.").

In short, once the false information about saved files is excised from the application and the true facts about Tor are added, there is no basis to conclude that copies of contraband pictures would have been found in Hawaii, let alone a year later in a different place. As a result, the issue in this case is not just whether the affidavit establishes that evidence was still on the premises by the time the search occurred. Rather, the affidavit misled the court about whether the evidence was ever present at all in Hawaii, and even more so as to its possible presence in Washington.

3. The Second *Franks* Violation: The False and Misleading "Collector Profile."

The affidavit also misled the court by including a false "collector profile." The profile is material because without it there is no basis for concluding that evidence or

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

contraband related to the alleged criminal activity in Hawaii would likely be found a year later in Washington. The profile was misleading in two critical respects.

First, the affidavit sought to connect the original Hawaii search location with the Washington search location through the profile by falsely asserting that "Tippens or a resident of the SUBJECT PREMISES displays characteristics" that fit the profile. Exh. A at ¶ 44 (capitalization in original). Without the profile, and in particular its assertion that such "collectors" keep contraband "for many years" (*id*. at ¶ 43(c)), the rest of the information in the affidavit is both stale and fails to establish a nexus between the alleged criminal activity and the location to be searched.

According to the Government itself, however, Tor users are not typical of child pornography offenders. To the contrary, the Government has maintained that Tor users are very different from the average Internet user and offender because they are technically sophisticated and highly attuned to security issues and possible detection. *See* exh. G; s*ee also, e.g., United States v. Michaud*, CR15-0531RJB. Dkt. 47 (Govt. Response to Motion to Suppress) at 25 (describing how Playpen was "no ordinary, run-of-the-mill website" and how its visitors are especially security minded and technically sophisticated).

Equally importantly, the Government has stated that Tor users are attentive to news about Internet investigations, share that information on Internet bulletin boards and in other forums, and are likely to conceal or delete evidence once an investigation becomes public. *Id*. In this case, news reports about Operation Pacifier began circulating in October 2015, and there were also reports about the FBI's use of NITs on the Tor network much earlier, long before the Washington search. *See also, e.g., United States v. Michaud*, dkt. 39 (Government's November 6, 2015, Response to Motion to Vacate or Modify Protective Order) at 4 (where it argued that, once the Playpen

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

investigation or the FBI's use of NITs became public, the targets may conceal or destroy evidence and jeopardize ongoing investigations).

None of that information was included in the instant warrant application, for the obvious reason that Tor users do not actually fit the profile that the Government presented. It would also have caused the issuing judge to focus more on the delay in seeking a warrant, which the profile was designed to minimize. Further, if the affidavit had included the characteristics of Tor users that the Government has alleged elsewhere, those characteristics would have weighed heavily against probable cause to believe that evidence was likely to be found in Washington.

The profile is also false and misleading for a reason directly related to the affidavit's misrepresentations about automatic downloading. *See* § II(A)(2), *supra*. Tor users, by utilizing the network security features that block automatic downloading, act in a way that is *inconsistent with* an intent to "possess, collect, receive, or distribute." *See* exh. B at ¶ 43 (a)-(e) and (g). They also act in a way that makes it *less* likely that they retain contraband, or any evidence that they viewed contraband, for any period of time, let alone for a year or more. Obviously, if someone wants to collect and retain child pornography on their computer, that person is unlikely to take affirmative steps to avoid receiving copies of the pornography. Since the affidavit contains no particular facts related to "Tippens or a resident" of the Hawaii house that might otherwise show a propensity to collect and retain (such as purchasing pornography, intentional downloading, or membership in non-Tor sites), the "collector profile" is not only irrelevant to the facts in this case, but affirmatively misleading.

The inclusion of this profile is particularly egregious because the Ninth Circuit long ago criticized "collector profiles" that consist of "boilerplate recitations designed to meet all law enforcement needs." *United States v. Weber*, 923 F.2d 1338, 1345 (9th Cir. 1990). In *Weber*, the Ninth Circuit held that "if the government presents expert

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

opinion about the behavior of a particular class of persons, for the opinion to have any relevance, the affidavit must lay a foundation which shows that the person subject to the search is a member of the class." *Id*. at 1345.

In this case, the Government presented one description of Tor users to the court in Virginia to support its applications for delayed notice authorizations, as well as oppose motions to unseal and make various other arguments here. *See* exh. F. It presented a different "profile" in the Washington affidavit that not only does not fit Tor users, but omitted all the facts that were inconsistent with that profile. As a result, the affidavit's profile not only fails to lay a foundation that shows that it relates to the relevant class; it also omitted all of the facts that were inconsistent with the conclusions that the Government wanted the court to draw about the target's habits and whether or not the particularized information was stale.

Indeed, even if this case did not involve Tor users, the collector profile would be essentially worthless. The malleability of the "expert" opinions that supposedly inform these profiles is demonstrated by the Government's recent reliance on an expert opinion that reached different conclusions about the typical person who views child pornography:

> Many users elect to view the files they download, get their gratification and then delete the files. Users who do this have either decided to do this out of fear of being caught by their significant other or out of a simpl[e] though[t] process [whereby] they [know] the files are out there and they can re-download them at anytime they want to get their next gratification. Some users feel guilty about their habits and discard all files and then when their need for gratification surpasses their guilt they download again.

Exh. H at 5 (excerpts of Government expert report and accompanying CV in *United States v. Hart*, CR14-5507RBL). The Government offered this expert opinion in a recent case where it needed to account for the absence of pornography on a computer, and it clearly would not serve the Government's purposes in the instant warrant

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

application. Here, rather than showing why pornography might not be found on a computer, the FBI had to persuade the court that it could still be found on a computer long after the alleged viewing. As a result, these cases offer a perfect example of how so-called profiles can be "designed to meet all law enforcement needs." *Weber*, 923 F.2d at 1345.

In *Weber*, the court reversed the denial of a suppression motion, and rejected the Government's assertion of "good faith," because the "foundationless" collector profile was material to finding probable cause to believe that evidence would be found at the defendant's home just four months after he had placed an order for apparent child pornography. *Id*. at 1346. Likewise, in this case the profile was material to determining probable cause to believe that evidence would be found in Washington, since without it there is no basis at all for concluding that it would be there, a year after the alleged viewing and thousands of miles from the place where it allegedly occurred.

In short, the "collector profile" was boilerplate; devoid of facts linking the profile to particular facts in the case; and inconsistent with expert opinions the Government has relied on in other cases. Most importantly, the profile is not relevant to Tor users, who the Government has elsewhere said have characteristics very different from the typical "collector" that are inconsistent with collecting contraband or storing inculpatory data on their computers for long periods of time. The Court should therefore excise the profile from the affidavit, which leaves only stale and misleading information about alleged downloading a year earlier at a different location.

4. The Third *Franks* Violation: The Missing Facts About Mr. Tippens' Relocation to Washington.

The affidavit was also intentionally or recklessly misleading because it did not disclose that Mr. Tippens' move from Hawaii to Washington was coordinated between the FBI and the Army and that the inventory of his property did not include a computer.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

The affidavit does not offer any basis for concluding that Mr. Tippens otherwise transported a computer to Washington. While many people have laptop computers, the affidavit does not suggest that "candygirl123" used a laptop or that Mr. Tippens owned one. In fact, it offers nothing to indicate that he had *any* computer, or even Internet access, at his new home.

Thus, even assuming that an excised and reformed affidavit establishes probable cause to believe that Mr. Tippens (or another resident of his Hawaii home) had viewed pornography in early 2015, there was no probable cause to believe that the target computer or related evidence would be found in Washington in 2016.

"The critical element in a reasonable search is not that the owner of the property is suspected of crime but that there is reasonable cause to believe that the specific things to be searched for and seized are located on the property to which entry is sought." *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978) (quotation marks omitted). Put another way, without a clear nexus between the location to be searched and the property that is sought, the warrant is invalid. *See, e.g., United States v. Grant*, 682 F.3d 827 (9th Cir. 2012) (reversing denial of suppression motion because, despite clear evidence of criminality, there was insufficient nexus between the residence and the evidence sought); *United States v. Hove*, 848 F.2d 137, 139 (9th Cir. 1988) (same).

Further, even when there is probable cause to believe that the items would have been found at the specified location at *some* time, there must be probable cause to believe they will be found there *at the time of the search*. Otherwise, the information will be deemed stale and the warrant is invalid. "While conclusive evidence of guilt is of course not necessary under this standard to establish probable cause, '[m]ere suspicion, common rumor, or even strong reason to suspect are not enough.'" *Torres v. City of Los Angeles*, 548 F.3d 1197, 1206-07 (9th Cir. 2008) (citations omitted).

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Some courts have given digital evidence a longer shelf life for probable cause purposes when there was also probable cause to conclude that the data would be found at a particular location. *See, e.g.*, *United States v. Hay*, 231 F.3d 630, 636 (9th Cir. 2000) (relying in part on affidavit's assertion that even if files were on a computer, they could be retrieved, even if deleted). Those cases are not relevant here, however, because the affidavit made false representations about whether files had been downloaded from Playpen in the first place. *See* § II(A)(2), *supra*. Hence, the affidavit not only recklessly or deliberately omitted the fact that Mr. Tippens' moving records show that he did not ship a computer to Washington, it also misled the court about whether the evidence detailed in the affidavit was likely present even before he was transferred.

Under these circumstances, there can be no credible dispute that the Magistrate Judge should have been presented with all the facts material to determining whether evidence of a crime allegedly committed in Hawaii was likely to be found much later in Washington. Given the false information contained in the affidavit about whether pictures had been downloaded from Playpen a year earlier; the lack of any information about whether there was a computer or even Internet service at the search location; and the absence of any other facts that might bridge the one-year gap between Hawaii and Washington, the property inventory weighs significantly against a finding of probable cause. And, since the FBI had received a copy of the inventory months before it applied for the warrant, the only explanation for its failure to disclose the inventory is that it is inconsistent with the conclusions that the FBI wanted the court to reach about the probability of finding evidence in Washington.

5. The Fourth *Franks* Violation: Omission of the FBI's Assessment of Whether it Would Actually Find Any Evidence if Mr. Tippens' Property was Searched.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

In the warrant application, the affiant states that he has probable cause to believe that contraband and evidence would be found at Mr. Tippens' home based not only on his own opinion and expertise, but the opinions and expertise of other agents who were familiar with the case. Exh. B at ¶¶ 5 and 6. These statements are important because the application involves novel and complex technical issues. Accordingly, the Magistrate Judge necessarily relied in large part on the FBI's conclusions about the reliability of the investigative techniques described in the application and the inferences that could be drawn from the computer activities that it describes.

While asserting reliance on the conclusions of others, the affiant misled the judge because he did not disclose that the FBI had previously concluded that there was insufficient evidence to proceed with a more timely search of Mr. Tippens' property. Specifically, the Chief Division Counsel in Hawaii memorialized the FBI's conclusions in correspondence with the Army's CID in September, 2015. The Chief Division Counsel serves as the top legal adviser for each FBI field office and, according to the FBI's job descriptions, his or her responsibilities include assessing "the legal implications" of any "technologies and techniques" used by the FBI, which presumably includes the implications of the "Network Investigative Technique" evidence as well. Consistent with that duty, Tony Lang, the Chief Division Counsel for the Honolulu field office, wrote to the CID that "any legal inference we can make about SFC Tippens viewing, downloading or manufacturing child pornography is extremely low and tenuous at best." Exh. D. The FBI communicated this assessment to CID after the Army had offered to postpone Mr. Tippens' transfer to Washington and search his property, which the Army was still in the process of moving. Exh. C.

At the time, the FBI had all of the information that the affiant would later summarize in the Washington warrant application. Specifically, the FBI had deployed its NIT months earlier and already collected all of the information about "candygirl123" that was included in that application.

Further, no new facts or information emerged after Mr. Tippens left Hawaii that might have added to probable cause. To the contrary, the only facts that developed

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

between the time that Mr. Tippens left Hawaii and the application in Washington are that he did in fact move; there was no evidence that he took a computer with him; and a substantial amount of additional time had passed. Moreover, the Chief Division Counsel was not just expressing his personal opinion about the available evidence, but spoke of the conclusions that "we" (i.e. the FBI, or at least the field office as a whole) had reached about the investigation.

The conclusions memorialized by the Chief Division Counsel are important because they are inconsistent with conclusions and inferences that the affiant did include in the Washington application, which is heavily reliant on expert opinions about the reliability of the NIT evidence and the legal inferences that can be drawn from it. As explained in *Stanert*, 762 F.2d at 781, "[b]y reporting less than the total story, an affiant can manipulate the inferences a magistrate will draw. To allow a magistrate to be misled in such a manner could denude the probable cause requirement of all real meaning." The omission of the Chief Division Counsel's conclusions are particularly material because, as noted, he is responsible for assessing the "legal implications" of the FBI's tools and techniques. It therefore appears that he, and others in the Hawaii field office as well, were less than confident about the reliability of the NIT evidence or the probability of finding evidence of a crime based on it, particularly since there were no other evidence establishing possible possession of contraband.

Equally importantly, "an officer's consultation with a government attorney is of significant importance to a finding of good faith." *United States v. Brown*, 951 F.2d 999, 1005 (9th Cir. 1991). Here, the Chief Division Counsel's conclusions were part of the FBI's case file, and the affiant therefore knew or should have known that the government attorney who had reviewed the evidence in the district where the alleged crime had occurred had concluded that the evidence that Mr. Tippens had viewed child pornography, let alone possessed it, was too tenuous to support a warrant. This fact should have been disclosed to the Magistrate Judge because it was material to her evaluation of the conclusions and inferences that the affiant did include. *Cf. United States v. Ryan*, 153 F.3d 708, 712 (8th Cir. 1998) (reflecting that district court

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

concluded and Government conceded that undisclosed opinion of Government expert, who disagreed with Government's other experts, was exculpatory under *Brady*, but concluding that disclosure would not have changed outcome); *Paradis v. Arave*, 130 F.3d 385, 395 (9th Cir. 1997) (finding *Brady* violation in failure to disclose that Government expert had previously had contrary opinion).

B. The Affidavit Fails to Establish Probable Cause that Evidence Would be Found at Mr. Tippens' Washington Residence.

Even without all the false statements and omissions, the Court should find that, given the totality of the circumstances, probable cause for a search of Mr. Tippens' home went from "extremely low and tenuous at best," as the FBI had concluded in September, 2015, to virtually nonexistent and entirely stale.

As a general matter, a warrant violates the Fourth Amendment if it is based on facts that are too remote in time to establish probable cause to believe that evidence will be found at the location to be searched. "[I]t is manifest that the proof must be of facts so closely related to the time of the issue of the warrant as to justify a finding of probable cause *at that time*." *Durham v. United States*, 403 F.2d 190, 193 (9th Cir. 1968) *(quoting Sgro v. United States*, 287 U.S. 206, 210 (1932)) (emphasis added).

Even "[t]he most convincing proof that the property was in the possession of the person or upon the premises at some remote time in the past will not justify a present invasion of privacy." *Durham*, 403 F.2d at 193. While the Ninth Circuit has upheld warrants that are based on information that may be relatively remote in time, in each case the affidavit demonstrated either a continuing pattern of suspicious activity or recent facts that corroborated and refreshed earlier illegal activity. Thus, in *Grant,* the Ninth Circuit held that "a 'mere lapse of substantial amounts of time,' does not undermine a warrant *if 'a continuing pattern or other good reasons' suggest that the evidence sought remains in the location to be searched*[.]" 682 F.3d at 835 (citation omitted). "In other words, because evidence can be moved or disposed of, the affidavit

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

must support an inference that it is presently in the residence to be searched, regardless of its past position." *Id*. This is particularly true here, where the Government has emphasized the time-sensitive nature of the Operation Pacifier searches because of the possible disposal or destruction of evidence once the operation became known. *See* exh. G.

Moreover, the lack of probable cause to search in Washington results not only from the prolonged passage of time and the distance between where the alleged connection to Playpen occurred and the search location. It also results from the fact that the evidence that the affidavit relies on (pictures purportedly downloaded from Playpen) was never in the "past position" either, since the affidavit misled the court about alleged downloading in the first place. *See* Section II(A)(2), *supra*.

Further, the affidavit does not allege that there was any "continuing pattern" or recent activity that might "freshen" the otherwise stale information. In fact, apart from establishing that Mr. Tippens lived at the new Washington residence, the affidavit contains no information whatsoever beyond what the FBI in Hawaii had concluded was "extremely low and tenuous at best" a year earlier.

It is also apparent that the FBI did not believe that Mr. Tippens had a continuing interest in child pornography, since it knew that he had custody of two minor children and not only decided not to pursue a warrant in Hawaii, but waited many additional months to apply for a warrant in Washington.[4]

---

[4] Given the FBI's lack of urgency (in contrast to that of Army investigators, who were pushing the FBI to obtain a timely warrant in Hawaii to help ensure the safety of Mr. Tippens' children), it is fortunate for the Bureau that Mr. Tippens is a loving and responsible parent. In this regard, his relationship with his daughters (ages 16 and 18) has been thoroughly investigated by Child Protective Services and law enforcement, which have concluded that he has taken good care of them. In addition, a polygraph examination has confirmed that Mr. Tippens has never had inappropriate contact with a child, and there is no allegation that he ever did. Mr. Tippens' children are now living with an aunt in Texas.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Finally, as discussed above, the Government has historically relied on a "collector profile" to try to compensate for otherwise stale information. The problem here is that the affidavit's collector profile is itself false and misleading. *See* section II(A)(3), *supra*. Perhaps most problematically, the Government has repeatedly claimed in other filings that Tor users are typically sensitive to detection and takes steps to avoid it; monitor the news and share information about Internet and Tor investigations; and may conceal, discard or destroy evidence once the Playpen investigation became public. Obviously, those characteristics make it far less likely that any evidence would be found by the time the FBI decided to search Mr. Tippens' Washington home, particularly since the FBI had shut Playpen down almost a year earlier and news of the Playpen investigation had been circulating widely. Yet none of these facts were included in the local warrant application.

With no other information linking the search location to the alleged crime, there is no probable cause to support the Washington warrant.

C. The "Good Faith" Exception Is Inapplicable.

The Government cannot invoke the good faith exception to rescue the affidavit. As noted earlier, the Government is foreclosed from relying on the exception when the affidavit includes false or materially misleading information, or omits material information. *Leon*, 468 U.S. at 923. The application is also patently defective given the lapse of time, the new and unrelated location of the search, and the lack of any evidence, apart from the boilerplate and false collector profile, that the target of the search was in fact a collector. *See Weber*, 923 F.2d 1338, 1345 (reversing denial of suppression motion, and finding no good faith, in part because "[i]t goes without saying that the government could not search Weber's house for evidence to prove Weber was a collector merely by alleging he was a collector.").

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

While warrant affidavits are not to be reviewed in a "hypertechnical" manner, they still must be carefully analyzed to ensure that the proposed inferences of probable cause to search in fact hold up. The Ninth Circuit decision in *Grant* is a good example of that. The Ninth Circuit concluded, as had the district court, that the affidavit did not establish probable cause that the items sought would be at the particular location. 682 F.3d at 832-35. The affidavit in *Grant*, thirteen pages with 50 exhibits,[5] contained a wealth of information purporting to link the premises to the cell phone that was sought. For example, the affidavit alleged that one of the homeowner's son's was connected to the gang suspected of being involved in the murder; had pawned the victim's Blackberry; had possessed the phone after the murder; and had possessed a gun looking like the murder weapon. *Id.* at 829-31, 832-33. The affiant also tied another son of the homeowner to the suspected gang, the description of the perpetrator, the city in which the crime had occurred, and another individual in contact with the victim's telephone after the murder. *Id.* at 829-31, 833-35. The affiant then attempted to link both sons with the homeowner and his residence. *Id.* at 829-31, 832-35.

The Ninth Circuit reviewed each thread of inference in detail to show that, when analyzed carefully, in fact there was insufficient validity to the inferences that the affiant wanted to draw. In *Grant*, there was no question that the affidavit established criminality; the weak link was the nexus of the particular premises to the items the warrant sought. *Id.* at 840.

The *Grant* court not only found a lack of probable cause, but also reversed the district court's ruling applying the good faith doctrine. *Id.* at 832-36. It did so despite the significant amount of information in the affidavit, and two separate potential links between the property and the gun that was sought. *Id.* at 832-35. The court concluded

[5] *See Government's Answering Brief*, No. 11-50036, 2011 WL 9680355, at *12 (9th Cir. Oct. 6, 2011).

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

that, despite all the information in the affidavit, ultimately there was no substance to the inference that the gun would be found at that particular location. The same conclusion applies to any inference that the instant affidavit established the presence of evidence at Mr. Tippens' home. *See also CDT*, 621 F.3d at 1177 (admonishing trial courts to be particularly attentive to inferences that the Government promotes in digital evidence cases and to exercise "greater vigilance" when reviewing warrants involving computer searches).

Finally, as previously noted, "an officer's consultation with a government attorney is of significant importance to a finding of good faith." *Brown*, 951 F.2d at 1005. The affiant in this case inevitably knew that the Chief Division Counsel in Hawaii had concluded that there were insufficient grounds to obtain a warrant to search Mr. Tippens' property, since that conclusion was made part of the case file.

IV. CONCLUSION

This Court should either suppress the fruits of the warrant or first grant a *Franks* hearing, after which it should suppress.

DATED this 26th day of January, 2017.

Respectfully submitted,

s/ *Colin Fieman*
Colin Fieman
Attorney for David Tippens

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

CERTIFICATE OF SERVICE

I hereby certify that on January 26, 2017, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to all parties registered with the CM/ECF system.

s/ *Amy Strickling, Paralegal*
Federal Public Defender Office

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710